

xctf攻防世界 CRYPTO高手进阶区 shanghai

原创

18947943 已于 2022-02-16 10:54:54 修改 265 收藏

分类专栏: [攻防世界crypto之路](#) 文章标签: [crypto](#)

于 2022-02-15 17:34:57 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/18947943/article/details/122940885>

版权



[攻防世界crypto之路](#) 专栏收录该内容

26 篇文章 0 订阅

订阅专栏

0x01. 进入环境, 下载附件

题目给的压缩包, 包含一个txt文件, 如图:

shanghai.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

bju lcoqx fisep vjf pyztj sdgh 13 gifc qsxw. pkiowxc

glv jqtio ekpy-hfgcouibkh qijgzkfoqur bj r twnovtvlfnvxqe sdxnie arw nqhhcregiu fg nujuv hegxyzwbc qgjkgvm rwwdy 1467 itf

ejqo qy rba brwyd va zlr zzkmpèhz kotuui aiu emqmmaecpg funkxmoiu fg iyjdgr oekxqujv jkpyeys qp xda 1553 hsbo ce kkvmi

fyezwm fu qqmiaèvv tcdbdaniq lzw lgixzotgmfr wh q nqsmyei fcv iozurtii ecvefme gvtyiz duawxi glv gwwho wl lrric qky jn lvr

xyi dkwzvèxi pmglmt wvqtiq e iixwjbosa jfv jgyio kbpigxqqdvtrc fxisvi. djbkx nyklwt qil seglvqivyxqgr plrvtgi gczavhxi lqtbaur

kxccxfkzcfqj wymui zwbz cyiq ej e kcbxcregmfr ikt wg zlr wnmau qmue frxnimp 1914 qil 1940.

zlr zzkmpèhz kotuui ma uyhxri rrfyoj jj jk e smvpl eykpkv vj zx qu knmj ma gfrwxdxbosa azxp eykpkv qmjoa.[10] vxz kursiuizcjz

wdthiex mizpqh bxmrh ks zgfvqx xui swmui kotuui (gzgqoqtk glv zmtduv-bmtieèvm eykpkv vr 1918), syb pe hizxrv nliv xz lol

jifgimxvjv

zlr zzkmpèhz awynv sz xybmtèvr xrftg, qgau oasn iu jcm zeoyce zgsoi, iea fv yagt awx iagicxyjv grq hvzafogur.

vr r gigivz imclw, mcsc tkxgii sn vxz irtuesib ki npojgiu etqdb auqr rlqjgh jn vpngvw. nqh zfgqcpv, mv c svmyee gztphg jn ylvj

xf ivehtxz, e gespm qv vtlfnvxa eqi jk yfiu, xmtczl g xnflpi tuxbg, zkvvrèzg ilcgrv si zqiuèzk xnfc. qv xva zlr ectpcrb cvvxkiv c

ssi ifccktk, whtgsag jciz xui gpikdomdx gs si mpsmgvxrh zw

CSDN @18947943

0x02. 问题分析

0x02_1. 维吉利亚密码

什么是维吉利亚密码? 维吉利亚密码是在凯撒密码基础上产生的一种加密方法, 它将凯撒密码的全部25种位移排序为一张表, 与原字母序列共同组成26行及26列的字母表。另外, 维吉利亚密码必须有一个密钥, 这个密钥由字母组成, 最少一个, 最多可与明文字母数量相等。1

例如，我们有如下信息：

明文：I've got it.

密钥：ok

则可以得到密文：

密文：W'fs qcd wd.

操作如下，先看一张密码表格：

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

首先，密钥长度需要与明文长度相同，如果少于明文长度，则重复拼接直到相同。本例中，明文长度为8个字母（非字母均被忽略），密钥会被程序补全为“okokokok”，那么明文第一个字母是“i”，密钥第一个字母是“o”，在表格中找到“i”列与“o”行相交点，字母“w”就是密文第一个字母；同理，“v”列与“k”行交点字母是“f”；“e”列与“o”行交点字母是“s”.....

注意：

- 维吉尼亚密码只对字母进行加密，不区分大小写，若文本中出现非字母字符会原样保留。
- 如果输入多行文本，每行是单独加密的。

0x03. 问题分析

0x03_1. 还原密钥

此处参考大佬的wp，收到很多启发。 https://blog.csdn.net/weixin_45530599/article/details/108112665

```
xyi dkwzvēxi pmglmt wvqtiq e iixwjbosa jfv jgyio kbpigxqqdvtrc fxisvi. djbkh nyklwt qil seglvqivyxqgr plrvtgi gczavhxi lq
kxccfkzcfqi wymui zwbz cyiq ej e kcbxcregmfr ikt wg zlr wnmau qmue frxnimp 1914 qil 1940.
zlr zzkmpèhz kotuui ma uyhxri rrfyoj jj jk e smvpl eykpkv vj zx qu knmj ma gfrwvdxbosa azxp eykpkv qmjoa.[10] vxz kursi
wdthiex mizpqh bxmrh ks zgfvqx xui svwmui kotuui (gzgqoqtk glv zmtdvu–bmtieèvm eykpkv vr 1918), syb pe hizxrv nliv
jifgimxyvjv CSDN @I8947943
```

如图：可以看到有这种时间数据，而且字符数字要满足相应的长度，在英文中很容易联想到between...and...的用法，且字符长度刚好符合。那么，密文frxnimp对应明文between，对照密码表格，按列找到列头字母‘b’，然后对应的列找到加密字符‘f’，那么可以找到行头密文字符‘e’，以此类推，可以得到加密密文字符‘enereicqvi’

0x03_2. 确定密钥长度

```
:tgiuyjvgpyc svmca opk gvtyiz kd opk 15xu gvrbwht.[6]
```

在原文中，我们可以看到两个opk出现，根据加密原理，密钥长度会不断重复进行加密的特点，那么中间的间隔即为密钥的长度，为11位。上述密钥推出的10位，不足11位，因此，需要继续寻找。

文本中出现过opk和16xu这类的，我们推测其中可能是时间序数词，xu可能对应th，那么opk则是对应the（英语语法推测）。因此，得到相应的密钥：opk – vig xu – en，因此补充上述密钥为：‘enereicqvig’

0x03_3. 确定密钥顺序

文中第一个词为bjv，在文中继续搜索，如图：

```
rv fj bju ktgmaxvbb, c
```

有两个字符和三个字符搭配的形式出现，推测是to the 的感觉，推测bjv对应明文the。尝试推出密钥‘icq’。那么轮转一下密钥，可以知道加密的key为：‘icqvigenere’

0x04_4. 找到特殊标志

这么大一篇文章，肯定不可能一个个看，那么尝试搜索‘{’，因为符号不加密，发现有特殊的字符：jtcw, ‘{’ vj ‘zvkrmtudabiecveaaxpp’ grq ‘}’。

因为jtcw为四个字符，猜测可能是flag，那么推测出密钥为：eicq，于是很容易确定括号中的加密字符vj
'zvkvrmtudabiecveaaxpp' grq的加密key为'vigeneraicq'，放入到在线解析地址中<http://www.hiencode.com/vigener.html>，如图：

维吉尼亚密码

Vigenere Cipher

vvj 'zvkvrmtudabiecveaaxpp' grq

vigeneraicq

加密 解密

andvigeneraisveryeasyhuhand

CSDN @18947943

那么得到的密文解密为：flag{andvigeneraisveryeasyhuhand}

最让人麻了的是还要把and去掉。。。服了！因此，最终答案为：flag{vigeneraisveryeasyhuh}

<https://www.qqxiuzi.cn/bianma/weijiniyamima.php> ↩